THE CLAIMS AS HEREIN AMENDED

1. (canceled)

2. (currently amended) A method according to claim ~~1~~ 20 wherein step B includes recording a PIN ~~number~~ as herein defined as part of the credit card information, and further wherein said PIN is included in said encrypted credit card information.

3. (canceled)

4. (currently amended) A method of conducting electronic credit card transactions so as to guard against fraud, comprising the following steps:

using an internet browser a user of a credit card issued by a credit card issuer ~~user~~ initiates a proposed credit card transaction with a third party vendor by accessing via said third party vendor a party authorized by said credit card issuer to validate credit card transactions and ~~validating institution via a third party vendor using an internet browser and~~ transmitting to said party ~~that validating institution~~ credit card information identifying said user and an encrypted date/time stamp representing the current transaction time ~~obtained from a non-adjustable time source~~;

said ~~validating institution~~ authorized party receives said encrypted date/time stamp and said other credit card information and decrypts said encrypted stamp to derive the current transaction time as represented by said decrypted date/time stamp;

said ~~validating institution~~ authorized party (1) compares said credit card information with previously recorded user information to verify that the user initiating the proposed transaction is an authorized user and (2) also compares the current transaction time represented by said decrypted

date/time stamp with the time of its receipt of said encrypted date time stamp and determines if the difference, if any, between said times is within a predetermined time limit; and

depending on the determination made in the foregoing step, the ~~validating institution~~ authorized party communicates to said third party vendor either a validation or rejection of ~~the transaction to the user initiating~~ the proposed transaction.

5. (currently amended) A method according to claim 4 wherein said user also transmits an encrypted PIN as herein defined to said ~~validating institution~~ authorized party via said third party vendor, and as part of its validation process said ~~validating institution~~ authorized party decrypts said PIN ~~as part of its validation process~~ and compares said decrypted PIN with user information previously recorded by said party to determine the validity of said decrypted PIN, and further wherein said authorized party rejects the proposed transaction if said decrypted PIN is not valid.

6. (currently amended) A method of providing security to an electronic credit card system wherein ~~initiation of~~ a credit card transaction involving a credit card user and a third party vendor requires ~~the credit card user to transmit~~ specific user-identifying information about the credit card user to be transmitted to a transaction-validating ~~institution~~ party via said third party vendor, comprising the step of including an encrypted date/time stamp as part of the credit card transaction information that is transmitted to the transaction-validating ~~institution~~ party via said third party vendor, said date/time stamp being derived from a non-adjustable time source and indicating the current time of the proposed transaction, said encrypted date/time stamp being encrypted according to an encryption scheme specified by said transaction-validating ~~institution~~ party.

7. (currently amended) A method according to claim 6 wherein said transaction information includes a credit card account number and a PIN as herein defined, and at least said credit card account number or said PIN is encrypted.

8. (canceled)

9. (canceled)

10. (canceled)

11. (currently amended) A method for authorizing an electronic business transaction by an authorized user, comprising the steps of:

(a) storing information about authorized users, including pre-set ~~unique identification codes~~ public key numbers and private key numbers for each authorized user, in a validating system, and providing said ~~identification codes~~ public and private key numbers to said authorized users for use in initiating and completing electronic transactions;

(b) receiving in the validating system for verification an encrypted ~~identification~~ code which is transmitted in connection with a proposed electronic business transaction at the request of a person who may or may not be an authorized user, said ~~identification~~ code ~~being transmitted and received together with~~ a comprising an encrypted date/time stamp representing the time that the proposed electronic business transaction was initiated by said person, a public key number and a private key number;

(c) decrypting said received encrypted code to retrieve said date/time stamp, said public key number and said private key number;

~~(c)~~ (d) comparing said ~~transmitted and received identification code~~ decrypted public and private key numbers with the pre-set unique ~~identification codes~~ public and private key numbers stored in said validating system to verify that ~~it is~~ they are valid, and rejecting the proposed

transaction if ~~said transmitted and received identification code is not valid~~ said decrypted public and private key numbers are not valid; and

~~(d).~~ (d) if said ~~transmitted and received identification code is~~ decrypted public and private key numbers are verified as valid, ~~(a)~~ (1) comparing the time represented by said decrypted date/time stamp with the time of receipt of said transmitted ~~identification~~ encrypted code ~~and date/time stamp~~ by said validating system, and ~~(b)~~ (2) rejecting the proposed transaction if there is a difference between the time represented by said decrypted date/time stamp and said time of receipt, and that difference exceeds a predetermined limit.

12. (currently amended) The method of claim 11 wherein said electronic ~~transactions~~ transaction is a credit card transaction, and ~~each of said unique identification codes include a unique~~ said public key number is a credit card account designation.

13. (currently amended) The method of claim 11 wherein said encrypted ~~identification~~ code received by said validating system is transmitted to said validating system via a third party vendor, and further wherein rejection or authorization of said proposed transaction is communicated by said validating system to said vendor.

14. (canceled)

15. (canceled)

16. (currently amended) The method of claim ~~15~~ 11 wherein said encrypted ~~transmitted and received identification~~ code includes ~~a~~ an encrypted PIN.

17. (canceled)

18. (currently amended) The method of claim 11 wherein said encrypted ~~transmitted and received identification~~ code includes ~~a~~ an encrypted PKN.

19. (canceled)

20. (new) A method of limiting the amount of time information pertaining to a credit card issued by a credit card issuer is valid for use in support of an electronic transaction with a vendor comprising the following steps:

A. a credit card user records credit card information required by the vendor via an internet browser, including credit card number, credit card expiration date, and the name of the credit card user;

B. a computer program provided by the credit card issuer or a party acting on behalf of said credit card issuer generates a date/time stamp representing the current date and time and encrypts said date/time stamp and at least some of said recorded credit card information;

C. said encrypted date/time stamp and said encrypted credit card information are transmitted from said credit card user via said vendor to a party authorized by the credit card issuer to validate proposed credit card transactions;

D. said party authorized by said credit card issuer to validate proposed credit card transactions conducts a validation process that comprises: (1) decrypting said encrypted date/time stamp and said encrypted credit card information, (2) determining if the age of the proposed transaction as represented by the time of the decrypted stamp is within a predetermined time limit required for validating the transaction, (3) comparing said decrypted credit card information with previously recorded credit card user information to verify that the party initiating the proposed credit card transaction is an authorized credit card user, and (4) depending on the determinations made

in foregoing steps (D)(2) and (D)(3), communicating either a validation or rejection of the proposed transaction to the third party vendor and/or the party who initiated the proposed credit card transaction.

21. (new) A method according to claim 20 wherein the date/time stamp is embedded in said credit card information.

22. (new) A method according to claim 20 wherein step B includes encryption of said credit card number.

23. (new) A method for conducting credit card transactions so as to guard against fraud, said method comprising steps as follows:

(a) a credit card user who proposes to carry out a credit card transaction with a third party vendor initiates the transaction by accessing a computer program supplied by the credit card issuer or a party acting on behalf of said credit card issuer that is constructed so as to (1) obtain a date/time stamp from a time source and (2) encrypt said date/time stamp and certain required credit card information identifying a credit card user;

(b) said credit card user supplies said certain required credit card information to said computer program and said computer program (a) obtains a date/time stamp in response to said certain credit card information and (b) generates an encrypted personal identification code comprising said date/time stamp and said certain required credit card information in encrypted form;

(c) said encrypted personal identification code is transmitted via said third party vendor to a validating system authorized to validate credit card transactions on behalf of said credit card issuer;

(d) said validating system decrypts said encrypted personal identification code to derive the current transaction time as represented by

the decrypted date/time stamp and said certain required credit card information in decrypted form;

(e) said validating system (1) compares said decrypted certain required credit card information with previously recorded user information to verify that the user initiating the proposed transaction is an authorized credit card user and (2) also compares the current transaction time represented by said decrypted date/time stamp with the time of its receipt and determines if the difference, if any, between said times is within a predetermined time limit; and

(f) depending on the determinations made in foregoing steps (e)(1) and (e)(2), the validating system communicates either a validation or rejection of the proposed transaction to the third party vendor and/or the party who initiated the proposed credit card transaction.

24. (new) A method according to claim 23 wherein said certain required information includes a credit card number and/or a private key number.

25. (new) A method according to claim 23 wherein said computer program is installed on the credit card user's computer containing a browser, and step (c) is conducted via the internet using said browser.

26. (new) A method according to claim 23 wherein said computer program is installed on a remote server and is accessed by said credit card user.

27. (new) A method for conducting electronic transactions so as to guard against fraud, said method comprising steps as follows:

(a) an entity who wishes to carry out an electronic transaction with a bank initiates the transaction by accessing a computer program supplied by said bank that is constructed so as to (1) obtain and encrypt a date/time

stamp in response to certain required information about the entity proposing to carry out the electronic transaction, and (2) encrypting said date/time stamp and said certain required information, said certain required information including an account number and a personal identification number representing said entity;

(b) said entity supplies said certain required information to said computer program and in response said computer program generates a date/time stamp and encrypts said date/time stamp and said certain required information;

(c) said encrypted date/time stamp and said encrypted certain required information are transmitted to and received by said bank or a validating party representing said bank;

(d) said receiving bank or validating party decrypts said received encrypted date/time stamp and said received encrypted certain required information;

(e) said receiving bank or validating party (1) compares said decrypted certain required information with previously recorded information to verify that the entity initiating the proposed transaction is an authorized entity and (2) also compares the transaction time represented by said decrypted date/time stamp with the time of its receipt by said bank or validating party to determine if the difference, if any, between said times is within a predetermined time limit; and

(f) depending on the determination made in steps (e)(1) and (e)(2), said bank or validating party communicates either a validation or rejection of the proposed transaction to the entity who initiated the proposed credit card transaction.

28. (new) A method according to claim 27 wherein in step (c) said encrypted date/time stamp and encrypted certain required information are transmitted to and received by said validating party, the steps in (e) are

carried out by the validating party, and in step (f) the validating party communicates said validation or rejection of the proposed transaction to said bank.